Haaga-Helia
ammattikorkeakoulu Oy

Identiteettivarkaudet ja niiltä suojautuminen

Susanna Marttila

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2018

Haaga-Helia ammattikorkeakoulu Oy

15.4.2018

Tekijä(t)
Susanna Marttila

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Identiteettivarkaudet ja niiltä suojautuminen

Sivu- ja liitesivumäärä
33

Opinnäytetyön otsikko englanniksi
Identity thefts and protection from them

Identiteetti on sarja asioita, jotka tekevät meistä tunnistettavia yksilöitä. Identiteettivarkaudessa ei varsinaisesti varasteta mitään, vaan varas lainaa toisen identiteettiä. Varkaudella pyritään usein saavuttamaan etuja tai hyödykkeitä, kuten myös identiteettivarkauksissa. Identiteettivarkaudessa varas pyrkii toisen identiteettiä käyttäen saamaan itselleen oikeudetonta etua tai hyötyä. Identiteettivarkauteen liittyy usein jokin muu rikos, kuten esimerkiksi petos.

Identiteetin voi varastaa kahdella tavalla: fyysisesti tai verkossa. Molemmat tavat avautuvat useammiksi alahaaroiksi. Fyysisiä keinoja on esimerkiksi luottokortin varastaminen, verkossa esimerkiksi salasanan ja käyttäjätilin kaappaaminen.

Opinnäytetyö pyrkii vastaamaan kysymyksiin mitä identiteettivarkaudet ovat ja miten niiltä voi suojautua. Keskeisenä kysymyksenä on selvittää, mitä identiteetti on ja mistä se muodostuu. Käsittelen opinnäytetyössäni myös tapoja varastaa identiteetti sekä suojautumisen tunnistamista ja keinoja hyödyntää suojautumista yksilön näkökulmasta. Opinnäytetyö tutkii oman ikäluokkani kykyä tunnistaa identiteettivarkauden uhat ja keinoja, joilla he ovat suojautuneet.

Identiteettivarkaus saattaa aiheuttaa uhrille taloudellisia ja henkisiä seurauksia. Identiteettivarkautta ja sen seurauksia voi olla vaikea havaita välittömästi. Seuraukset voivat ilmetä vasta vuosia varkauden jälkeen esimerkiksi tietovuodon seurauksena. Seurauksia voivat olla esimerkiksi luottotietojen menetys tai henkilökuvan murentuminen työelämässä.

Suojautuminen on sarja keinoja ja huolellisuutta. Suojautumisessa oleellista on ymmärtää, mitä jakaa ja minne ja kenelle oikeuksia omiin tietoihinsa antaa. Tietojen huolellinen säilytys ja hävittäminen auttavat arjessa identiteettivarkaudelta suojautumiseen.

Asiasanat
Identiteettivarkaus, biotunnistus, tietoturva

Sisällys

1 Johdanto

Opinnäytetyössä perehdyn sosiaalisessa mediassa, verkossa ja fyysisesti tehtäviin identiteettivarkauksiin, joissa tietoja käyttäjästä kerätään ja myydään erilaisilla menetelmillä. Työ perustuu tutkimukseen, jossa kartoitetaan miten helposti käyttäjät ovat valmiita luovuttamaan tietojaan, millaisia hankaluuksia identiteettivarkaudesta on, millaisia tietoja identiteettivarkaat keräävät, millä keinoilla tietoja kerätään sekä mitä seurauksia identiteettivarkaudesta on.

Opinnäytetyössäni jätän käsittelemättä mobiilimaksamisen ja siihen liittyvät identiteettivarkauksien mahdollisuudet sekä syvällisemmän perehtymisen mainonnan algoritmeihin ja niihin liittyviin identiteettivarkauksiin. Jätän myös käsittelemättä varsinaisen päätelaitteeseen hakkeroimisen ja haittaohjelmat. Aihe on ajankohtainen ja siitä kertyy koko ajan lisää tietoa, jonka vuoksi perehdyn ainoastaan laaja-alaiseen yleiskatsaukseen identiteettivarkauksista ja niiltä suojautumiseen.

Tutkimuksen tarkoituksena on valistaa aktiivisia sosiaalisen median käyttäjiä jakamiensa tietojen väärinkäyttömahdollisuuksista sekä selvittää, minkälaista tietovarastoa harmittoman tuntuisista tiedoista huijarit luovat käyttääkseen tietoja väärin. Perehdyn myös ongelmiin, joita identiteettivarkaus tuo. Tutkimus tarjoaa tapoja muuttaa käyttäytymistään, mikäli epäilee oman identiteettinsä tai tietojensa olevan vaarassa joutua vääriin käsiin.

Opinnäytetyö pyrkii vastamaan laajempaan kysymykseen, mitä identiteettivarkaudet ovat ja miten niiltä voi suojautua. Työssä selvitetään myös yleisimpiä tapoja varastaa identiteetti sekä selvitetään keinoja, joita yksityishenkilö voi tunnistaa ja hyödyntää oman identiteettinsä suojaamiseen.

2 Identiteettivarkaus ja siihen liittyvä tiedon kerääminen

Identiteettivaras pyrkii selvittämään uhristaan mahdollisimman kattavasti tietoja käyttääkseen niitä väärin. Rikoksen tekijä käyttää tekoonsa yksilöiviä tietoja (Åberg 2017, 114).

2.1. Identiteetti, mistä se muodostuu?

Suomen kieleen sana identiteetti on johdettu latinan kielen sanasta ”identitas, idem”, joka tarkoittaa ”samaa”. Filosofiassa ja psykologiassa identiteetti määritellään hieman eri tavoin. Filosofisesti sana määrittelee laadullista kuvausta kyseessä olevasta oliosta ja olion pysymisestä samanlaisena ajankohdasta toiseen. Ihmisten kohdalla identiteetti määrittyy

vastaamalla kysymykseen ”kuka hän on?”. Identiteetti tarkoittaa olion pysymistä samanlaisena eli tunnistettavana yhdestä hetkestä toiseen jolloin se voidaan tunnistaa samaksi olioksi tunnusmerkkien perusteella. (Tieteen termipankki, 3.4.2018.)

Jotta olisimme tunnistettavia henkilöitä, jotta minä olisin minä, täytyy minussa olla jotakin, joka erottaa minut muista. Tällaisia seikkoja ovat esimerkiksi ulkonäkö, nimi, syntymäpäivä, sosiaaliturvatunnus, dna ja sormenjäljet. (Tietosuojavaltuutetun toimisto, 2010.) Näistä ainoastaan sosiaaliturvatunnuksen loppuosaa voi muuttaa, mutta helppoa se ei ole (Tietosuojavaltuutetun toimisto, 2010).

Tieteen näkökulmasta tarkasteltuna identiteetti on melko tiukasti määritelty olion pysymisenä samanlaisena yhdestä hetkestä toiseen (Tieteen termipankki, 3.4.2018). Tietosuojavaltuutetun toimiston antamassa määrittelyssä identiteetin luomiseen taas riittää esimerkiksi ulkonäkö sekä keinotekoiset nimi ja sosiaaliturvatunnus (Tietosuojavaltuutetun toimisto, 2010).

Voidaan siis päätellä, että nimeä voi vaihtaa ja ulkonäköään muuttaa, mutta tiettyjä tunnistettavia ulkonäöllisiä piirteitä meissä silti voi olla. Yksilöivät seikat ovat siis toisaalta paras tunnistuksemme – ne ovat henkilökohtaisia ja yksityisiä, kun puhutaan esimerkiksi sormenjäljestä. Toisaalta ne ovat paras ase meitä vastaan väärissä käsissä. Keinotekoisesti luotuja pankkitunnuksia, salasanoja, käyttäjätunnuksia ja muita kirjautumismenetelmiä voidaan aina luoda lisää ja muuttaa, mutta biometrisiä tunnisteita ei voi muuttaa.

2.2 Identiteettivarkaus ja sen kriminalisointi

Identiteettivarkaus kriminalisoitiin 4.9.2015 rikoslakiin (Hallituksen esitys 232/2014). Kun identiteettiä käytetään uhrin tietämättä, mutta ei varasteta uhrin käytöstä, on kyse identiteettivarkaudesta (Kangasniemi 2012, 217). Identiteettivarkaudesta puhuttaessa puhutaan siis siitä, että toinen henkilö oikeudettomasti ottaa käyttöönsä toista henkilöä yksilöiviä tietoja, kuten henkilötietoja, salasanoja, pankkitunnuksia tai kirjautumistunnuksia (Åberg 2017, 114–115).

Rikoslain 28 luvun 1 §:n mukaan varkaudessa on kyse irtaimen omaisuuden anastamisesta toisen hallusta. Aineetonta omaisuutta ei siis yleisesti ottaen voi anastaa. (Kangasniemi 2012, 217.) Koska identiteetti on aineetonta, ei sitä voida varastaa rikoslaissa määritellyn varkauden tavalla:

> ”Joka anastaa toisen hallusta irtainta omaisuutta, on tuomittava varkaudesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi kuudeksi kuukaudeksi.” (RL, 19.12.1889/39, luku 28, 1 §).

Identiteettivarkaudessa ei siis suoranaisesti varasteta mitään fyysisesti, vaan esiinnytään toisena henkilönä. Rikoksentekijän tarkoituksena on erehdyttää kolmatta osapuolta esiintymällä jonakin toisena henkilönä. Rikoksentekijä voi käyttää tarkoitukseensa esimerkiksi henkilötietoja, tunnistautumistietoja tai muita yksilöiviä tietoja. (Åberg 2017, 114.)

Keväällä 2017 Helsingin Sanomat uutisoi identiteettivarkauden kriminalisoinnin jälkeen rikosilmoitusten määrän kasvaneen räjähdysmäisesti. Vuonna 2015 rikosilmoituksia tehtiin koko maassa 534 kun vuonna 2016 niitä tehtiin 3303. (Pajuriutta 25.2.2017.)

Yleensä identiteettivarkauteen liittyy siis jokin toinen rikos, useimmiten petos. Tietoja on käytetty hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä kuten Suomen Rikoslain luvussa 36 1 § on säädetty.

> ”Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava *petoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Petoksesta tuomitaan myös se, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa. Yritys on rangaistava.” (RL 24.8.1990/769, luku 36, 1 §.)

Identiteettivarkaus on siis nimikkeenä harhaanjohtava. Muita termejä ei kuitenkaan ole juurikaan käytössä suomen kielessä. Englannin kielestä käännöksenä sen sijaan voisivat olla esimerkiksi ”identity fraud” eli identiteettipetos tai ”identity cloning” eli identiteetin kopioiminen. (Puro 2017, 8.)

Suomen rikoslain 38. luvussa 9 a § määrittelee toisen henkilötietoja, tunnistamistietoja tai vastaavia yksilöiviä tietoja oikeudettomasti käyttävän sekä taloudellista vahinkoa tai vähäistä suurempaa haittaa aiheuttavan tuomittavaksi identiteettivarkaudesta sakkoon (RL, 19.12.1889/39, luku 38, 9 a §).

Yhteisenä tekijänä eri lähteistä nousi esiin, että mikäli taloudellista tai sosiaalista haittaa ei synny, ei rikosilmoitusta yleensä ymmärretä tehdä eikä tekoa voida kriminalisoida. Lainsäädäntö tuntuu laahaavan perässä, sillä keinoja anastaa toista yksilöiviä tietoja tuntuu olevan lukemattomia, samoin kuin keinoja aiheuttaa niillä vahinkoa ja taloudellisia menetyksiä. Digitaalinen maailma myös muuttuu niin nopeasti, ettei lainsäädäntö ehdi mukaan.

2.3. Tietojen kerääminen fyysisesti

Perinteinen tapa on kerätä uhrista perus- ja henkilötietoja, kuten nimi, osoitetiedot, pankkitiedot, luottokortin tiedot, sosiaaliturvatunnus tai puhelinnumero. Identiteettivarkaus tapahtuu tällöin usein oikeassa elämässä varastamalla postia, passi, lompakko tai muulla fyysisellä varkaudella. (mySafety, Research Insight Finland, 31.5.2017.)

Nimi- ja osoitetiedot riittävät yleensä jo joihinkin verkkokauppoihin, varsinkin kun tilausten summa pysyy pienenä. Kun näihin tietoihin lisätään vielä henkilötunnus, on rikosten tekeminen helppoa. (Karismo 15.2.2017.) Henkilöpapereistaan, kuten passista tai ajokortista ei missään tapauksessa kannata laittaa kuvaa sosiaaliseen mediaan, josta tiedot käyvät ilmi. Myös syntymäpäivän ilmoittaminen helpottaa todellisen henkilöllisyytesi päättelemistä. (Tranberg & Heuer, 2013, 228.)

2.4. Tietojen kerääminen sähköisesti

Verkossa tehtävä identiteettivarkaus tarkoittaa esimerkiksi sosiaalisen median tilin kaappaamista ja siellä esiintymistä toisena henkilönä. Viruksin ja hakkeroimalla tehtävät tunkeutumiset uhrin laitteeseen ovat myös identiteettivarkauksia, kun tietoja kerätään esimerkiksi näppäilytallennuksin tai tallennettujen salasanojen muodossa. (Poliisi, Tietorikoksia.)

Tietoja saatetaan myös kalastella verkossa esiintymällä esimerkiksi pankin edustajana. Esimerkiksi Aktia muistuttaa, ettei pankki koskaan pyydä verkkopankkitunnuksia sähköpostitse. (Aktia 2018.) Yritysten välisessä kaupankäynnissä huijari saattaa esiintyä myyjänä tai tavarantoimittajana ja lähettää tekaistuja viestejä, joissa ilmoitetaan maksutietojen vaihtuneen ja pyydetään maksamaan huijarin tilille (Poliisi, Sähköpostihuijauksia).

Sähköistyvän ja digitalisoituvan maailman myötä toisen henkilötietojen varastaminen ja käyttäminen on tullut yhä helpommaksi. Tiedot saatuaan väärinkäyttäjä saattaa tilata uhrin maksettavaksi tavaroita ja palveluita internetistä tai saattaa jopa tyhjentää pankkitilin. Maailmalla identiteettivarkauksien uskotaan olevan nopeimmin kasvava rikollisuuden muoto. (Niiniluoto, 2015.)

2.4.1. Tietojen kerääminen sosiaalisesta mediasta

Oletko törmännyt Facebookissa testeihin, jotka selvittävät vaikkapa keneltä julkisuuden henkilöltä näytät tai mikä seuraava sukunimesi tulee olemaan? Testien periaate on käyttää Facebook-tiliä ja kysyä joitakin tarkentavia tietoja, kuten äidin tyttönimeä. Harmittomilta tuntuvien testien tekeminen sosiaalisen median palveluissa on helppoa, mutta emme tiedä, mihin luovutettuja tietoja voidaan myydä ja mitä kaikkea niillä voi tehdä. Myös Facebook-kavereiden tiedot altistuvat väärinkäytölle. Testit ovat ensisijaisesti hupia ja viihdyttäviä. Tämä lisää niiden koukuttavuutta. Tietojen kertominen Facebook-kavereille ja tästä saatavat tykkäykset ja kommentit lisäävät entisestään koukuttavuutta, koska niillä saamme kaipaamaamme huomiota. Testien tulosta voidaan myös haluta vertailla kavereiden kanssa. (Kähkönen, 29.3.2016.)

Yleensä palveluntarjoajan sivulla on kerrottu selvästi, että käyttäjä antaa yritykselle luvan hyödyntää antamiaan tietoja. Ennen testin tekemistä käyttäjä yleensä huolettomasti klikkaa hyväksy-nappia miettimällä tarkemmin mitä tietoja antaa käytettäväksi. Hyväksymällä ehdot käyttäjä luovuttaa myös oikeuden myydä tietojaan kolmannelle osapuolelle. Tärkeä kerättävä tieto on sähköposti, johon voidaan kohdentaa mainontaa. Hyväksymättä ehtoja ei pääse jatkamaan, jonka vuoksi on houkuttelevaa hyväksyä ehdot. (Kähkönen, 29.3.2016.)

Johtopäätöksenä voidaan todeta, että tietoja yhdistelemällä saadaan laaja kokonaisuus. Esiinnymme sosiaalisessa mediassa useimmiten omalla nimellämme. Lisäksi profiilissamme saattaa olla profiilikuva, joka on esimerkiksi työpaikalle otettu virallinen kuva, jossa näkyvät hyvin kasvot. Syntymäpäiväonnitteluja tulvii Facebookissa ilmoitettuna syntymäpäivänämme, syntymäaika kokonaisuudessaan voi olla näkyvillä tai pääteltävissä profiilista. Profiilistamme selviää työpaikka ja ammatti, työpaikan sivulta tai numeropalvelusta numero ja mahdollisesti myös osoite. Jo näin harmittomalla tiedon jakamisella väärin käsiin voi joutua koko identiteettimme, pahimmassa tapauksessa sitä voidaan käyttää jopa väärennetyn passin tekemiseen.

2.4.2. Verkkokaupparikollisuus

Identiteettivarkaus ei ole ainoa rikos, vaan yleensä tapahtumaan liittyy myös muu rikos – useimmiten petos, kun tavaroita tilataan toisen henkilön nimiin. Kun rikolliselle on selvää, missä verkkokaupassa henkilö on jo asioinut, saattaa hän saada helposti tilattua sieltä lisää. Osaan verkkokaupoista on lisätty palvelu, jolla asiakaskokemus paranee: automaattiset maksutiedot. Kaikkia tietoja ei siis tarvitse joka kerta täydentää. Tämä helpottaa tietojen väärinkäyttöä, jos osa tiedoista on jo saatu. (Karismo, 15.2.2017.)

Suosittu tapa sekä kerätä tietoa, että saada huijatuksi maksamaan, on tarjota jotakin niin houkuttelevasti, että siihen on helppo tarttua. Maksamalla pienen summan, jopa euron, ja täyttämällä yhteys- ja luottokorttitietonsa henkilölle uskotellaan vastineeksi saapuvan esimerkiksi uuden älypuhelimen. Tarkoituksena on kuitenkin ainoastaan kerätä tietoa ja veloittaa luottokortilta muita, kalliimpia tilauksia. (Karismo, 15.2.2017.)

Ongelmana identiteettivarkauksissa on, ettei uhri tiedä mistä ja milloin tiedot on anastettu. Tietoja saatetaan säilöä pitkiäkin aikoja ennen väärinkäyttöä. Tietoja myös myydään järjestelmällisesti eteenpäin, osa markkinointiin ja osa rikolliseen käyttöön. (Hämäläinen & Tuominen, 5.11.2017.)

Facebookissa esiintyvien arvontojen ja kilpailujen avulla kerätään myös paljon tietoja. Joskus nämä ovat tunnettujen yritysten nimissä tehtäviä, mutta huijauksia. Arvonnan oikeellisuus on hyvä varmistaa yrityksen virallisilta sivuilta. (Forss 2014, 93.)

3 Biometriset tunnisteet ja identiteetin varastaminen

Biometristen tunnisteiden avulla identiteetin varastaminen on uhrille hankalampaa ja rikolliselle arvokkaampaa, koska biometrisiä tunnisteita ei ole luotu keinotekoisesti kuten salasanoja ja käyttäjätunnisteita (Keränen 2016.)

3.1. Mitä biometriset tunnisteet ovat

Biometrisistä tunnisteista yleisimmin tunnettu on varmastikin sormenjälki, joka on käytössä monilla älylaitteen lukituksen avaamiseksi. Myös passiin on jo pidemmän aikaa vaadittu sormenjäljet Euroopan Unionin passiasetuksen mukaisesti. Toinen biometrinen tunniste lisättiin vuonna 2006, kun passin siruun lisättiin kasvokuva. (Suomen Suurlähetystö, Moskova.)

> ”Biometrinen tunnistus tarkoittaa sitä että henkilö tunnistetaan käyttäen hyväksi ihmisruumiin ainutlaatuisia piirteitä, biometrisiä tunnisteita, joita ovat esimerkiksi ihmisen sormenjäljet. Vain hyvin harvoilla ihmisillä on samanlaiset biometriset tunnisteet, joten niiden avulla ihminen voidaan tunnistaa lähes varmasti. Yleisimmin käytettyjä biometrisia tunnisteita ovat kasvot, ääni, sormenjäljet, silmän iiris, kämmenen muoto sekä perinteinen allekirjoitus.” (Tietosuojavaltuutetun toimisto, 2010.)

Niiden käyttämisessä on selviä etuja: niitä ei voi unohtaa kotiin, tunnistuslaitteiden huijaaminen on hankalaa ja tunnistautuminen koetaan helpommaksi kuin salasanalla tapahtuva tunnistautuminen (Tietosuojavaltuutetun toimisto, 2010).

3.2. Biometristen tunnisteiden haitat

Sormenjälkiämme, dna:ta, ääntä tai silmän iiriksiä emme voi vaihtaa. Niitä voidaan kuitenkin kerätä ja käyttää tunnistautumiseen huomaamattamme. Väärinkäyttöä voi olla hyvin vaikeaa estää tai havaita ennalta. Biometrisiä tunnisteita tulisikin käyttää yhdessä perinteisten tunnistusmenetelmien kuten avainten ja salasanojen kanssa. Tietojen säilyttämistä tulee myös miettiä tarkoin ja esimerkiksi dnasta saatavia perimä- ja terveystietoja ja niiden käsittely tulee turvata ja tietojen määrää tulee kontrolloida. (Tietosuojavaltuutetun toimisto, 2010.)

Biometriset tunnisteet tekevät identiteettivarkauksista yhä arvokkaampia ja kasvattavat bisnestä. Biometrinen tunniste on yhdistettävissä vain yhteen ihmiseen maailmassa, joka tekee tiedoista erittäin arkaluontoisia. Pelkkää biometristä tunnistetta käyttävä järjestelmä on haavoittuva. Jos käyttäjä käyttää useissa toisistaan riippumattomissa järjestelmissä samaa biometrista tunnistetta, olisi sen menettäminen identiteettivarkaalle erittäin haitallista. Kuten muissakin tunnistejärjestelmissä, biometrisen tunnisteen käyttäminen itsessään on turvallista. Datan ja rekistereiden pitäminen sen sijaan tekee siitä vaarallista. Toukokuussa voimaan astuva Euroopan Unionin tietosuoja-asetus katsoo biometriset tunnisteet erityiseksi henkilötietojen ryhmäksi ja asettaa niiden käsittelysäännöt paljon tiukemmiksi kuin tavallisissa henkilötiedoissa. (Keränen 2016.)

Yates (2016) listaa kolme syytä, joiden vuoksi sormenjälkeä ei tulisi käyttää tunnisteena. Ensimmäisenä syynä mainitaan sormenjäljen varastamisen helppous. Niitä jää kaikkialle – ovenkahvoihin, laseihin, näyttöihin ja lukemattomiin muihin paikkoihin. Sormenjäljen voi myös muodostaa keinotekoisesti esimerkiksi ottamalla valokuvan uhrin sormesta. Pahempaa tietysti on, että sormenjälki voidaan hakkeroida.

Toisena syynä mainitaan itsestäänselvyys: salasanaa voimme vaihtaa, sormenjälkiämme emme. Joten jos ne päätyvät väärään käyttöön, ne myös pysyvät siellä. Kolmantena syynä on Yhdysvaltojen lainsäädäntö, joka antaa viranomaisille oikeuden määrätä avaamaan puhelin, mikäli se liittyy rikostutkintaan ja on lukittu sormenjäljellä, joka katsotaan fyysiseksi todisteeksi. (Yates 2016.)

4 Identiteettivarkaudesta aiheutuvat ongelmat

Identiteettivarkauden kriminalisointi on tärkeää uhrin kannalta. Uhri voi kokea ahdistusta ja turvattomuuden tunnetta rikoksen aiheuttaman harmin ja vaikeusten lisäksi. Uhrista tilanne voi tuntua hallitsemattomalta, koska varastetun identiteetin kaikkia käyttötarkoituksia ei tiedetä tai mitä sillä voidaan vielä tulevaisuudessa tehdä. Rikoksesta aiheutuu usein sekä taloudellista että henkistä vahinkoa. Varastetulla identiteetillä tehdyistä teoista voi joutua kärsimään jopa vuosia. (Åberg 2017, 115.)

Rikosuhripäivystys voi auttaa, jos joutuu rikoksen uhriksi tai epäilee sellaista, läheinen on joutunut rikoksen uhriksi tai on vaikkapa todistajana rikoksessa. Rikosuhripäivystys opastaa muun muassa rikosilmoituksen tekemisessä, kertoo, miten prosessi etenee ja keneltä saa henkistä tukea. (Rikosuhripäivystys 2018.)

5 Identiteettivarkaudelta suojautuminen

Suojautuminen on lopulta hyvin yksinkertaista, vaikka saattaakin aluksi tuntua monimutkaiselta. Mitä vähemmän tietoa itsestään ja esimerkiksi lapsistaan ja kodistaan jakaa, sitä paremmin on suojattu. Verkossa ei pidä tehdä mitään sellaista, mitä ei tekisi myös reaalielämässä. (Peltomäki & Norppa 2015, 82.) Mikäli ei ymmärrä, mistä todella on kyse, ei pidä osta mitään tai luovuttaa tietojaan (Peltomäki ym. 2015, 83). Kuluttajaan kohdistuva verkkorikos tapahtuu yleensä laitteen kautta. Tietokoneeseen tulee yleensä virus vahingossa, älypuhelin taas saastuu käyttäjän huolimattomuuden vuoksi. (Peltomäki ym. 2015, 85)

5.1. Toiminta identiteettivarkauden sattuessa

Jos epäilee, että identiteetti on varastettu tai henkilötietoja käytetään väärin, tulee välittömästi tehdä rikosilmoitus. Rangaistavaa voi olla myös muun rikossäännöksen nojalla, joten rikosilmoituksen saatuaan poliisi ratkaisee, millä rikosnimikkeellä asiaa tutkitaan. (Åberg 2017, 115.)

Jos henkilötietoja käytetään väärin, voi tehdä omaehtoisen luottokiellon. Virallisille tahoille, kuten Väestörekisterikeskukseen, maistraattiin ja Postiin on hyvä ilmoittaa oikeat osoitetiedot ja henkilötietojen väärinkäytöstä. Todisteet, kuten tilausvahvistukset ja laskut pitää säilyttää todisteina. Petoksen kohteina oleviin organisaatioihin kannattaa ottaa yhteyttä ja tehdä tarvittaessa reklamaatio.

Mikäli henkilötietoja käytetään kiusaamiseen tai häiriköintiin, kannattaa valeprofiilin poistoa pyytää sosiaalisen median palveluista, hakukoneista ja muista palveluista ja rekistereistä. Osoitetietonsa voi varmistaa oikeiksi Väestörekisterikeskukseen, maistraattiin ja Postiin. Jos epäilee, että tilille on tunkeuduttu, tulee salasana vaihtaa välittömästi. Jos mahdollista, tarkista missä palveluun on kirjauduttu ja miltä laitteelta.

Jotkin palvelut mahdollistavat aktiivisten kirjautumisten tarkastelun. Sulje kaikki kirjautumiset ja muista tarkastaa myös tiliin liitetyt palvelut, kuten Facebook-tilillä Instagramiin kirjautuminen. Vaihda salasana kaikkialle, jossa käytät samaa tunnusta tai salasanaa. Tarkista tiliisi liitetyn salasanan palautuksen sähköposti oikeaksi. Pyydä tarvittaessa apua palveluntarjoajalta tilisi palauttamiseen. Kerää todisteita esimerkiksi ruutukaappauksin. Ole yhteydessä poliisiin ja tee rikosilmoitus.

Maksukortin väärinkäytöksissä on tärkeää sulkea maksukortti välittömästi sulkupalvelussa ja ilmoittaa väärinkäytöstä kortin myöntäjälle. Kerää tiedot rikosilmoitusta varten luvattomista maksutapahtumista. Tee maksukorttiyhtiölle oikaisupyyntö luvattomista maksuista. Jos luvattomaan maksutapahtumaan liittyy kolmas osapuoli, ota yhteyttä palveluntarjoajaan ja vaadi maksun kumoamista. (Åberg 2017, 115-116.)

5.2. Keinot identiteettivarkaudelta suojautumiseen

Järvinen kuvaa kirjassaan hyvin suhdettamme puhelimeen. Lapsille iskostetaan, että pitää olla aina tavoitettavissa ja aikuisetkin vilkuilevat kokouksessa puhelintaan. (Järvinen 2010, 25.) Toisaalta taas meitä kehotetaan ottamaan etäisyyttä digimaailmaan (Tranberg ym. 2013, 103). Yhteenvetona voidaan todeta, että teknologian kehittymisestä on meille paljon hyötyä, mutta samalla se asettaa meille uusia haasteita.

5.2.1. Puhelin tai muu älylaite

Mitä vähemmän puhelimessasi on toimintoja, sitä turvallisempi se on. Jos et tarvitse internettiä, GPS-paikannusta tai sähköpostia puhelimeen, hanki tavallinen peruspuhelin. Sijaintipalveluiden perusteella sinua voidaan seurata ja jäljittää. Älä asenna älylaitteeseesi turhia sovelluksia. (Järvinen 2010, 35.)

Mieti, mitä lataat: onko sovellus aito ja kenen tekemä se on? Onko sillä muita käyttäjiä? Lue myös muiden käyttäjien arvosteluja. Mieti myös, mihin palveluihin ja sovelluksiin kirjaudut käyttäen Facebook- tai Twitter-tiliäsi. Päästät samalla sovelluksen osittain tai kokonaan sosiaalisen median tilillesi. (Tranberg ym. 2013, 243.) Säilytä puhelimesi mukana

tullut IMEI-koodi, joka on laitteen sarjanumero. IMEI-koodi on sekä laitteen pakkauksessa, että itse laitteessa. (Järvinen 2010, 35.)

Älä anna puhelintasi tuntemattomille tai jätä sitä valvomatta – siihen voidaan asentaa helposti seuranta- tai salakuuntelulaite. Käytä suojakoodia sisäänkirjautumiseen ja aseta sille aktivointiaika, jonka päätyttyä laite menee automaattisesti uudestaan itse lukkoon. Älä aseta syntymäpäivääsi PIN-koodiksi. Se liittyy usein liittymätietoihisi ja on helppo saada selville. Yleisimmät PIN-koodit ovat 1234 ja 0000. (Järvinen 2010, 35.)

Käytä ajantasaisia, päivitettyjä ohjelmaversioita, ne ovat yleensä tietoturvaltaan parhaita. Asenna virustorjunta ja huolehdi, että se pysyy ajan tasalla. Valitse hyvät salasanat, joista lisää kappaleessa 5.3. Rajoita päätelaitteisiin pääsyä: mitkä sovellukset ja yhteydet sinulla on käytössä? Mieti, mitä klikkaat ja avaat. (Peltomäki & Norppa 2015, 86.)

5.2.2. Tietokone

Tyhjennä selaimen välimuisti, sivuhistoria ja evästeet ainakin säännöllisesti tai mieluiten joka kerran jälkeen. Jos viet laitettasi huoltoon, tyhjennä tallennetut salasanat ja ota esimerkiksi ulkoiselle kovalevylle talteen sellaiset tiedot, joihin et halua päästää muita käsiksi. Myös varmuuskopio on hyvä tehdä. Peitä tietokoneen videokamera silloin, kun et käytä sitä. Käytä julkisella tai vieraalla tietokoneella yksityistä selainta. Tätä voit käyttää myös henkilökohtaisella laitteellasi. Muista, ettei selailusi silti ole täysin salattua.

Säädä selaimen asetuksista historian pituus, välimuistin koko ja evästeiden hallinta sopivaksi. Kokeile myös evästeiden automaattista poistoa. Jos käyttö poiston jälkeen hankaloituu, palauta asetukset takaisin. Käytä Firefox -selaimella master-salasanaa, joka suojaa muut salasanat. Jos haluat käyttää selailuun Chromea, valitse SRWare, joka poistaa kaikki ylimääräiset Googlen kehittämät, käyttäjän seurantaa helpottavat ominaisuudet.

Älä anna sähköpostiohjelmasi ladata automaattisesti viestien kuvia, niiden mukana voi tulla haittaohjelmia. Älä käytä Flash-laajennusta, ellet ehdottomasti tarvitse sitä. Flashissa on suuria tietoturva-aukkoja. Älä luovuta tietojasi Euroopan Unionin ulkopuolelle. (Järvinen 2010, 174, 195.) Käytä vain ajantasaisia, päivitettyjä ohjelmaversioita. Ne ovat kaikkein turvallisimpia. Asenna virustorjunta ja pidä huolta sen päivityksistä.

Valitse hyvät salasanat ja käytä niitä. Käytä myös eri salasanoja eri paikoissa. Salasanoista lisää kappaleessa 5.3. Rajoita päätelaitteisiin pääsyä: sovellukset ja yhteydet. Mitkä

sovellukset sinulla on käytössäsi? Poista turhat sovellukset ja tarkista asetuksista, millä sovelluksilla on pääsy tietoihisi. Mieti, mitä klikkaat ja avaat. (Peltomäki ym. 2015, 86.)

5.2.3. Sosiaalinen media

Laita sosiaaliseen mediaan vain sellaista aineistoa, jonka olet valmis näyttämään kaikille. Yksityisyysasetuksista huolimatta materiaalia on helppo levittää muille ja kerran nettiin laitettua ei saa koskaan pois. Hyvä mittari on miettiä, näyttäisitkö materiaalia pomollesi tai vanhemmillesi. Pidä Facebook-profiilisi julkisena. Silloin on helppo muistaa, että kuvat ja postaukset näkyvät kaikille. Toinen vaihtoehto on pitää hyvin rajattua kaveripiiriä ja tiukasti yksityistä profiilia. Älä käytä Facebookin lisäohjelmia, kuten kyselyitä, pelejä tai testejä. Ohjelmilla on esteetön pääsy henkilötietoihisi. Verkoston analysointia voi hämätä joko pitämällä ystäväpiirin mahdollisimman pienenä tai hyväksymällä kaikki kaveripyynnöt, jolloin ystäväpiiristä ei enää voi tehdä päätelmiä. (Järvinen 2010, 239.)

5.2.4. Fyysinen tietoturva

Käytä lukittavaa postilaatikkoa. Postilaatikostasi voidaan varastaa henkilötietojasi sisältävää postia tai esimerkiksi pankin lähettämiä pankkitunnuksia. Jos olet poissa kotoa, pyydä jota kuta tyhjentämään postilaatikkosi. Mitä pidempään säilytät postia laatikossa, sen suurempi riski varastamiselle on. Täysinäinen postilaatikko saattaa myös viestiä murtovarkaille, että talo on tyhjä. Seuraa pankkien ja luottoyhtiöiden lähettämää postia ja varmista, että saat kaikki postit, joita sieltä pitäisi tulla.

Älä heitä pois sellaisia papereita, joissa on henkilökohtaisia tietojasi. Tällaisia ovat esimerkiksi pankin tiliotteet tai laskut. Revi paperit pieniksi paloiksi ja laita vaikkapa eri roska-astioihin, jolloin väärinkäyttäjän on vaikeampi muodostaa niistä palapeli. Hae kotiosoitettasi ja henkilötunnustasi netistä eri selaimilla yksityisessä tilassa. Mikäli tietosi löytyvät, pyydä järjestelmän ylläpitäjää poistamaan ne. (Järvinen 2010, 278.)

5.3. Salasanat

Salasanoja kaapataan esimerkiksi kolmella tavalla: hyökkääjä lähettää koneeseen haitta-ohjelman, joka tallentaa näppäinkomentoja, lähettämällä ilmoitus salasanan vanhenemisesta ja lisäämällä paluuosoitteeksi oman osoitteensa tai käymällä merkkiyhdistelmiä läpi kunnes oikea löytyy. Hyvässä salasanassa on ä- ja ö-kirjaimia, isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.

Salasanan on hyvä olla myös riittävän pitkä ja monimutkainen. Isoja kirjaimia kannattaa sijoittaa keskelle, samoin kuin numerot. On havaittu, että useista sanoista koostuva salasana on vahva. Jokaisessa palvelussa olisi hyvä olla erilainen salasana ja salasanaa tulisi vaihtaa riittävän usein. (Peltomäki ym. 2015, 91.)

5.4. Identiteetti

Tarkista säännöllisesti maineesi verkossa. Hae itseäsi eri hakukoneilla ja eri selaimilla sekä mieluiten myös incognito-tilassa. Voit käyttää myös Google Alerts –palvelua, joka hälyttää ja lähettää sähköpostin aina kun asettamiasi hakusanoja (esimerkiksi oma nimi) esiintyy verkkosivuilla tai julkaisuissa. On olemassa myös muita tilaajapohjaisia seuranta- ja puhdistuspalveluita.

Jos löydät itsestäsi hakutuloksia, jotka eivät pidä paikkaansa tai ovat ikäviä, voit koettaa saada alkuperäisen lähteen korjaaman tiedon tai luoda runsaasti uutta tietoa, jotka saavat muita hakutuloksia putoamaan hakutuloksissa alaspäin. Käytä kuitenkin apunasi hakukoneoptimoinnin, Search Engine Optimization, ammattilaista avuksesi. Jos huomaat henkilötietojasi olevan verkossa ja etenkin tietoja kokoaviin palveluihin, voit pyytää palvelun ylläpitäjältä tietojesi poistoa.

Älä koskaan julkaise henkilötunnustasi verkossa. Henkilötunnusta ei tule ilmoittaa millään digitaalisella alustalla, ansioluettelossa, sähköpostissa tai kuvassa. Älä kirjoita sitä keskustelupalstoille, kahden keskeisiin viesteihin esimerkiksi chatissa tai yhteisöpalveluissa ja vältä myös sähköpostiin kirjoittamista. Luovuta henkilötunnuksesi vain yrityksille, joihin luotat.

Ottaessasi käyttöön uusia palveluita tai sovelluksia, anna vain pakolliset vaaditut tiedot. Tarkista, ettei uusi palvelu saa käyttöönsä kontaktilistojasi, jolloin varjelet myös ystäväpiiriäsi roskapostilta ja tietojenlouhinnalta. Älä hyväksy suoraan tuntemattomien kaveripyyntöjä tai yhteydenottopyyntöjä. (Tranberg ym. 2013, 244-246.)

6 Ajankohtaisia tapauksia tosielämästä

6.1. Tapaus Facebook ja Cambridge Analytics

Vuoden 2018 alussa sattui ehkä suurin tietovuoto nyky-yhteiskunnan älylaitteiden ja sosiaalisen median parissa. Sosiaalisen median jätti, Facebook, myönsi jopa 87 miljoonaa ihmistä koskevan tietojen jakamisen poliittiselle konsulttiyritykselle Cambridge Analyticsille.

Cambridge Analytics on aiemmin liitetty aiemmin kahteen poliittiseen pommiin: Iso-Britannian äänestykseen pois Euroopan Unionista eli Brexitiin sekä vuoden 2016 Yhdysvaltojen presidentinvaalien voittajaan Donald Trumpiin. (BBC, 4.4.2018.)

Kumpikin oli aiemmin asiantuntijoiden ja gallupien mukaan päättymässä toisin – brittien odotettiin pysyvän Euroopan Unionissa ja Yhdysvaltojen presidentiksi odotettiin Hillary Clintonia. Yllättäviä vaalituloksia on selitetty yksilöllisesti kohdennetulla kampanjoinnilla. Menettelyä on pidetty jopa demokratian uhkana. Kumpaakin vaalipommia yhdistää kaksi asiaa – Big Data ja Cambridge Analytics. Big Datalla tarkoitetaan tietoja, joita meistä jää viesteistämme, tiedonhausta, palveluiden käytöstä ja ostoksista verkossa. Kohdennettu markkinointi tarkoittaa juuri näiden tietojen hyödyntämistä, eli autoja selailevalle mainostetaan autoihin liittyviä mainoksia.

Yhdysvaltalainen yhtiö, Cambridge Analytics, suunnittelee ja toteuttaa kohdennettua mainontaa poliittisiin mainoskampanjoihin. Cambridge Analytics toteutti myös Donald Trumpin vaalikampanjan. (Hyytinen, 29.4.2017).

Guardian kertoi ennen Donald Trumpia republikaanien presidenttiehdokkaana olleen Ted Cruzin käyttäneen Cambridge Analyticsiä tekemään psykologisesti kohdennettua vaalikampanjaa, jossa Facebook-käyttäjien henkilökohtaista dataa käytettiin ilman heidän lupaansa tai tietoaan. (Davies, 11.12.2015).

Tietoja oli kerätty vapaaehtoisilta Cambridgen yliopiston tutkimukseen, jossa Facebook-tykkäyksien perusteella määrittelee persoonallisuuden piirteesi, älykkyytesi, poliittiset ja uskonnolliset näkemykset ja seksuaalisen suuntautumisesi. Tutkimusaineistoa kertyi miljoonista ihmisistä. Hyvään tarkoitukseen annettuja tietoja Cambridge Analytics käytti törkeästi hyväkseen. (Hyytinen, 29.4.2017.)

Maaliskuussa 2017 ilmeni, että Facebookin dataa on jaettu Cambridge Analyticsille. Myöhemmin Mark Zuckerberg, yhteisöpalvelu Facebookin perustaja ja toimitusjohtaja, myönsi toisen ison ongelman. Ominaisuutta, jonka avulla käyttäjät voivat etsiä toisiaan puhelinnumeron tai sähköpostin avulla, on käytetty väärin. Väärinkäytön myötä useiden ihmisten julkisia profiilitietoja on ”kaavittu” ja yhdistetty yhteystietoihin, jotka on saatu muualta. (BBC, 4.4.2018.)

Facebook on luovuttanut jopa 2,7 miljoonan eurooppalaisen tietoja Cambridge Analyticsille. Euroopan Unionin komissio selvittää asiaa Mark Zuckenbergin kanssa. Cambridge

Analytics on käyttänyt tietoja brexit-kampanjaan ja Donald Trumpin vaalikampanjaan. (Kokkonen, 6.4.2018).

Tapaus on mielenkiintoinen, koska se osoittaa kuinka valtavia vaikutuksia tietovuodoilla voi olla. Tapauksessa ei puhtaasti ole kyse identiteettivarkaudesta vaan sen lieveilmiöstä. Identiteettiä on kuitenkin käytetty väärin äänestystulokseen vaikuttamiseksi.

6.2. Tapaus Amanda Kastrup

Alkuperältään tanskalainen, Nicole N. Horianyn ohjaama dokumenttielokuva kertoo Amanda Kastrupista, jonka elämä muuttuu kertaheitolla hänen tavattuaan Facebookissa Casperin. Amandaa lähestyy Facebookissa nainen ja lyhyen keskustelun jälkeen Amanda alkaa jutella naisen ”serkun”, Casperin, kanssa.

Casper kertoo olevansa rikkaan suvun vesa ja pyytää Amandaa googlettamaan perhesäätiön todistaakseen henkilöllisyytensä. Casper Augustinus on tosiaankin olemassa. Pian Casper muuttaa Amandan luo. Casper soittaa siltatullista ja sanoo, ettei hänen luottokorttinsa toimi. Hän kysyy lupaa nostaa autosta löytämältään Amandan kortilta rahaa. Amandalle soitetaan pankista ja käy ilmi, että Casper on toimittanut sinne valtakirjan, joka valtuuttaa hänet nostamaan Amandan nimissä 13.500 euron pankkilainan sekä hankkimaan kaksi luottokorttia, joiden luottoraja on ylitetty.

Pankista kehoitetaan Amandaa tekemään välittömästi rikosilmoitus Casperista, tai velat kaatuvat Amandan niskaan. Samalla Amandalle selviää, ettei hänen poikaystävänsä ole lainkaan se henkilö, jona hän on esiintynyt ja asunut Amandan kanssa. Amandalle selviää, ettei Casper Augustinus olekaan Casper Augustinus, vaan Casper Rieper-Holm.

Amanda tekee rikosilmoituksen poliisille. Myös Amandasta on tehty rikosilmoitus ennen kuin selviää, että häntäkin on huijattu. Poliisi on etsinyt Casperia.

Googlettaessaan Casper Rieper-Holmia, Amanda ymmärtää, ettei ole ainoa huijattu. Hakutulokset antavat useita kertomuksia huijarista ja paljastaa Casperin käyttäneen useita eri henkilöllisyyksiä.

Casper on huijannut muun muassa Slagelsenin käsipalloseuraa. Tanskan liigassa pelannut seura oli konkurssin partaalla, kun amerikkalaisen miljonäärin pojanpoikaa esittänyt Casper ilmaantui pelastamaan sen. Rahoja ei kuitenkaan koskaan ole ollut olemassakaan.

Lopussa selviää, ettei tytärtä, ei ystäviä, ei perhettä, ei ketään Casperin luomista hahmoista ole ollut olemassakaan. Kaikki Facebook-profiilit ovat valeprofiileja. Casperilta oli jäänyt Amandan puhelimeen henkilökohtaisia puhelinnumeroita ja Amanda soittaa niihin. Hän keskustelee muiden naisten kanssa, joita Casper on huijannut.

Amanda soitti myös Casperin äidille. Selvisi, että milloin Casper ei huijannut, hän asui isovanhempiensa kanssa heidän talonsa kellarissa. Hän auttoi isovanhempiaan mutta huijasi myös heitä kerta toisensa jälkeen ja valehteli kahdentoista vuoden ajan, että hänellä on tytär. Tytärtä ei kuitenkaan ollut olemassa. Casperin huijaukset ulottuivat myös Tanskan rajojen ulkopuolelle.

Nordea ja Hotelli Skodsborg haastoivat Casper Rieper-Holmin oikeuteen ja Amanda Kastrup todisti häntä vastaan. Syytetty tuomittiin viimeisen 10 vuoden aikana tehdyistä vastaavista rikoksista vuodeksi vankeuteen. Amandan, Nordean ja Hotelli Skodsborgin tapaus oli neljästoista.

Tapauksessa oli merkittävää se, kuinka monien ihmisten identiteetin Casper Rieder-Holm varasti huijatakseen Amandaa. Rieder-Holm oli luonut kokonaisen verkoston Facebook-tilejä ja puhelinnumeroita myöden ”ystäviä ja perheenjäseniä” itselleen. Hän oli myös varastanut oikean Casper Augustinuksen henkilöllisyyden, Amanda Kastrupin henkilöllisyyden väärentäessään valtakirjan ja syyllistyi samalla useisiin muihin rikoksiin. Tekijä on tässä toiminut erityisen häikäilemättömällä tavalla lyöttäytyessään uhrin kotiin asumaan. Tapahtumia on vaikea uskoa todeksi, mutta taitava huijari on saanut useita ihmisiä kiedottua verkkoonsa. (Horiany 2017; Det Danske Filminsitut 2017; Jyllands-Posten 2009; Christiansen 2009.)

7 Biometristen identiteettivarkauksien uhkakuvat

Jo vuonna 2005 tehdyssä liikenne- ja viestintäministeriön selvityksestä käy ilmi, että biometristen tunnisteiden ongelmat ovat säilyneet samankaltaisina tähän päivään asti (Taulukko 4). Jo tuolloin on kiinnitetty huomiota identiteettivarkauteen, vaikka se onkin kriminalisoitu useita vuosia myöhemmin. Suomessa meillä on vahva usko viranomaisten vilpittömyyteen, mutta taulukosta käy ilmi, että eräs uhkakuva on myös viranomaisten saama liika tieto. Julkisessa keskustelussa tunnetuimpia uhkakuvia ovat olleet yhteiskunnan kohtuuton valvonta ja seuranta (Big Brother -ilmiö), identiteettivarkaudet ja biometrian huijaaminen (Taulukko 4).

Taulukko 4 Identiteettivarkauden uhkakuva (Ailisto, Ahonen & Lindholm 15.11.2005)

Uhkakuva	Selite tai esimerkki
Vallan keskittyminen	”Tieto on valtaa”, esim. Viranomaiset tai yritystahot saavat kohtuuttomasti valtaa keräytyvän tiedon ja yhdistelyn kautta
Kerätyn tiedon käyttö muuhun tarkoitukseen	Esimerkiksi bio-passikuvatietojen käyttö katu- tai liikennevalvonnassa
Biometrisen tiedon vuotaminen	Vrt. Luottokorttinumeroiden vuotaminen internettiin, -> uhka esim. Sormenjälkitietojen kohdalla laittomien kopioiden valmistus ja rikollinen käyttö
Biometrisen tiedon myyminen	Sama kuin yllä
Ihmisen arvon ja yksityisyyden kunnioittamisen rapautuminen	Kuluttaja voi antaa biometrisen tunnisteen vähäistä taloudellista etua, esimerkiksi pientä alennusta tai lahjaa, vastaan harkitsematta seurauksia
Identiteettivarkaus	Varkaus voi tapahtua enrollauksessa, ts. henkilö A esiintyy henkilönä B ja ”syrjäyttää” hänen identiteettinsä TAI henkilö A kopioi henkilön B tunnisteen, esimerkiksi sormenjäljen, väärentää sen ja käyttää sitä
Identiteettihuijaus	Kuten yllä, mutta henkilö B osallistuu huijaukseen
Syrjäytyminen	Henkilöt, jotka eivät voi, osaa tai halua käyttää biometrisia tunnisteita esimerkiksi fyysisen vamman, oppimiskyvyn puutteiden, uskonnollisen tai muun vakaumuksen takia ovat vaarassa jäädä joidenkin palvelujen, etujen tai alennusten ulkopuolelle
Liiallinen luottamus	Biometrista tunnistusta käyttävä yritys, viranomainen tai niiden työntekijät tai suuri yleisö luottaa sokeasti biometriseen tunnistukseen, ts. sen oletetaan olevan 100% varma.

Taulukossa 5 on selvennetty seurauksia uhrin kannalta sekä torjuntakeinoja. Taulukon perusteella voitaneen päätellä, että luotettavia ja tyydyttäviä torjuntakeinoja on vaikea löytää. Taulukossa olisi ehkä ollut myös hyvä vertailla, kuinka hyviä eri keinot ovat tunnistukseen. Parhaimmalta tavalta kuitenkin vaikuttaa biometrisen ja fyysisen tunnisteen yhdistelmä, eli esimerkiksi sormenjälki ja kulkukortti.

Taulukko 5 Identiteettivarkauden uhkakuvat eri järjestelmillä (Ailisto ym. 15.11.2005).

Järjestelmän luonne	Seuraus uhrin kannalta	Torjuntakeinot ja niiden luotettavuus
Pelkkä biometrinen tunniste	Käytetty biometria menettää käyttökelpoisuutensa järjestelmässä	1) Biometrisen tunnisteen ”mitätöinti” pysyvästi. Luotettava, mutta ei tyydyttävä keino. 2) Aitouden (liveness) varmistus anturissa. Ei koskaan täysin luotettava, asiantuntijan huijattavissa. Olemassa olevan laitekannan ongelma.*
Biometrinen tunniste ja kortti tms. tunniste.	Uhka, jos kortti varastetaan yhtä aikaa biometrian kanssa.	Kortin mitätöinti. Luotettavuus kortin turvatason mukaan, yleensä hyvä.
Biometrinen tunniste ja PIN tai tunnussana Biometrinen tunniste ja keskusrekisteri	Uhka, jos PIN myös luvattoman käyttäjän tiedossa. Käytetty biometria menettää käyttökelpoisuutensa järjestelmässä.	PINin vaihto. 1) Biometrisen tunnisteen ”mitätöinti” pysyvästi. Luotettava mutta ei tyydyttävä keino. 2) Aitouden (liveness) varmistus anturissa. Ei täysin luotettava, asiantuntijan huijattavissa.
Useita biometrisia tunnisteita ja keskusrekisteri (esim. sormenjälki ja kasvokuva kuten passissa voi tulevaisuudessa olla).	Haittavaikutus ei niin suuri kuin yllä.	Ihmisen tekemä tunnistus varmistaa (käytännössä kasvot).

*Aitouden varmistus ja huijauskeinot käyvät kilpajuoksua, jota voi verrata virusten ja virustorjuntaohjelmien vastaavaan. Koska aitouden (aliveness) tunnistus on paljolti laitteistopohjaista, ei päivitys ole läheskään niin helppoa kuin virustorjunnan kohdalla. Vanha laitekanta on altista uusille huijauskeinoille.

8 Tutkimus sosiaalisen median käyttäjien kokemuksista

Tutkimusmenetelmänä käytetään kyselyä sosiaalisessa mediassa Google Forms-työkalun avulla. Vastaajat olivat noin 20-50-vuotiaita miehiä ja naisia. Valitsin tutkimusmenetelmäksi avoimen kyselyn saadakseni mahdollisimman kattavan otannan vastauksia. Vastaajia oli yhteensä 164. Kysymykset perustuvat teoriapohjaan.

Tutkimukseni on kvantitiivinen eli määrällinen tutkimus. Kvantitatiivisessa analyysissa argumentoidaan lukujen ja niiden välisten yhteyksien avulla (Alasuutari 1994, 25). Kvantitatiivinen ja kvalitatiivinen tutkimus eivät kuitenkaan sulje toisiaan täysin pois, sillä niillä on yhteisiä periaatteita kuten pyrkimys loogiseen todisteluun (Alasuutari 1994, 23). Lisäksi käytössä on case-tutkimus, jossa kysytään miten ja miksi jotakin tapahtui jossakin tietyssä tapauksessa (Järvinen & Järvinen 2000, 8-9).

Tutkimuksella pyrin selvittämään, miten hyvin sosiaalisen median käyttäjät tuntevat riskit identiteettivarkauteen ja miten he ovat suojautuneet sitä vastaan. Tutkimuksen tulosten toivon voivan auttaa muuttamaan omia toimintatapoja yhä turvallisempaan verkon käyttöön sekä fyysiseen identiteetin suojaamiseen. Tuloksia tutkailemalla lukija voi saada käsityksen siitä, millaisia eri keinoja hänen tulisi omassa elämässään käyttää välttyäkseen identiteettivarkaudelta.

8.1. Käytätkö eri salasanoja eri järjestelmissä?

Kyselyyn vastanneista suurin osa, 76,7 %, käyttää eri salasanoja joissakin eri palveluissa. 20,3 % käyttää kaikissa palveluissa eri salasanaa ja pieni osa, 3,1 % käyttää kaikissa samaa. Jokaisessa palvelussa olisi hyvä olla erilainen salasana ja salasanaa tulisi vaihtaa riittävän usein (Peltomäki ym. 2015, 91).

8.2. Poistatko evästeitä ja selailuhistoriaa?

64,1 % poistaa evästeitään ja selailuhistoriaansa. Selvästi pienempi osa, 35,9 % ei poista evästeitä ja selailuhistoriaansa. Evästeet ja selailuhistoria olisi hyvä poistaa säännöllisesti. Selainhistoria paljastaa melkein kaiken käyttäjästä. Evästeillä selain tunnistaa käyttäjän ja

voi suunnata esimerkiksi kohdennettua mainontaa selailuhistorian perusteella. (Järvinen 2010, 164, 172, 174.)

8.3. Käytätkö selainta incognito-tilassa? (yksityistä selainta)

60 % käyttää joskus, 20 % ei koskaan, 13,8 % ei ole koskaan kuullut tällaisesta ja 6,2 % käyttää aina selainta yksityisen selaamisen tilassa. Yksityinen tila minimoi selailusta syntyvät jäljet, uudet evästeet poistetaan automaattisesti selainta suljettaessa. On hyvä muistaa, ettei yksityinen selaaminen ei suojaa käyttäjää nettipalveluihin tai verkkoon päin. (Järvinen 2010, 172-173.)

8.4. Onko älylaitteesi suojattu sormenjäljellä tai muulla biometrisellä tunnisteella? (esimerkiksi kasvojentunnistus)

67,7 % käyttää biometristä tunnistetta älylaitteensa suojaamiseen. 24,6 % ei käytä ja 7,7 % laitteessa se ei ole mahdollista. Biometristen tunnisteiden käyttämisessä on selviä etuja: niitä ei voi unohtaa kotiin, tunnistuslaitteiden huijaaminen on hankalaa ja tunnistautuminen koetaan helpommaksi kuin salasanalla tapahtuva tunnistautuminen (Tietosuojavaltuutetun toimisto, 2010). Biometrinen tunniste on yhdistettävissä vain yhteen ihmiseen maailmassa, joka tekee tiedoista erittäin arkaluontoisia. Pelkkää biometristä tunnistetta käyttävä järjestelmä on haavoittuva. (Keränen 2016.) Biometrinen tunniste on asiantuntijan huijattavissa (Ailisto ym. 15.11.2005.)

8.5. Onko laitteesi (=älylaite, tietokone) suojattu salasanalla tai pääsykoodilla?

92,3 % laite on suojattu salasanalla tai pääsykoodilla, vain murto-osa, 7,7 % ei käytä suojausta. Ilman suojakoodia oleva laite on todella haavoittuva. Suojakoodille tai salasanalle kannattaa asettaa aktivointiaika, jonka päätyttyä laite menee automaattisesti uudestaan itse lukkoon. Älä aseta syntymäpäivääsi PIN-koodiksi. Se liittyy usein liittymätietoihisi ja on helppo saada selville. Yleisimmät PIN-koodit ovat 1234 ja 0000. (Järvinen 2010, 35.)

8.6. Onko laitteessasi (=älylaite, tietokone) virustorjunta?

Valtaosalla, 87,7 % on laitteessaan käytössä virustorjunta. 7,7 % ei ole ja 4,6 % ei ole varma. Ajantasainen ja päivitetty virustorjunta on paras keino suojautua viruksilta. Lisäksi kannattaa miettiä, mitä klikkaa, millä sivustoilla käy ja millaisia sovelluksia asentaa. (Peltomäki ym. 2015, 86.)

8.7. Oletko tallentanut luottokorttisi tietoja automaattisiin tallennuksiin? (esimerkiksi verkkokaupassa, josta olet jo aiemmin tilannut, luottokorttisi numero tulee automaattisesti maksuvaiheessa tai mobiilimaksamiseen)

Lähes puolet, 44,6 % ei ole tallentanut maksutietojaan. 24,6 % on tallentanut mobiilimaksamiseen, 16,9 % on tallentanut sekä verkkokauppaan että mobiilimaksamiseen ja 13,8 % ainoastaan tuttuun verkkokauppaan.

Verkkomaksamisessa kannattaa käyttää luotettavien toimijoiden maksukortteja, kuten Visan tai MasterCardin verifioimia kortteja. Voi myös käyttää virtuaalisia kortteja, joihin ladataan haluttu summa rahaa. (Peltomäki ym. 2015, 84.) Luottokortti- tai pankkitietoja ei pidä syöttää sivulle, ellei osoite ala https-määreellä (Peltomäki ym. 2015, 97). Vuonna 2013 noin 60 prosenttia maksuvälinepetoksista johtuvista tappioista Euroopan Unionin maissa johtui korttidatan varastamisesta sähköisistä palveluista. Älylaitteen arvo kasvaa mobiilimaksamisen myötä, koska maksutiedot ovat laitteessa itsessään. Harva lainaa luottokorttiaan tuntemattomalle, mutta älylaitteen kanssa emme osaa olla yhtä varovaisia. Mobiilimaksaminen kasvattaa tietoturvavaatimuksia. (Peltomäki ym. 2015, 122). Tallennetut korttitiedot ovat helposti väärinkäytettäviä, jos palvelun salasana saadaan selville.

8.8. Oletko tallentanut osoitetietojasi automaattisiin tallennuksiin? (täyttäessäsi lomakkeita tietosi täydentyvät automaattisesti)

78,5 % on tallentanut osoitetietonsa automaattisiin tallennuksiin, 21,5 % ei ole tallentanut. Automaattisesti täydentyvät lomaketiedot helpottavat ja nopeuttavat toki esimerkiksi verkkokaupasta tilaamista, mutta tietoja tallentaessa ei ehkä tule mieleen, minkä tietoturvariskin samalla ottaa. Emme tarkasti tiedä, mihin kaikkialle tiedot päätyvät ja tietoja on helppo käyttää väärin.

8.9. Käytätkö Google Alertsia henkilötietoihisi koskeviin hälytyksiin?

49,2 % ei ole koskaan kuullut Google Alertsista, 33,8 % ei käytä ja 16,9 % käyttää hälytyksiä itsestään.

Google Alertsiin voi määritellä omat henkilötietonsa jonka jälkeen ohjelma lähettää sähköpostin, aina kun tiedot mainitaan verkossa. Näin voi valvoa, mitä itsestään kirjoitetaan ja missä. Hälytyksen voi asettaa haluamilleen hakusanoille. (Tranberg ym. 2013, 244-246.)

8.10. Oletko koskaan jakanut henkilötunnuksesi loppuosaa sosiaalisessa mediassa? (esimerkiksi kuvassa näkyvässä passissa, todistuksessa tai muussa sellaisessa)

Lähes kukaan, 95,4 % ei ole jakanut, 1,5 % on jakanut ja 3,1 % ei ole varma. Henkilötunnuksen avulla voi tehdä lukemattomia rikoksia, kuten tilata toisen nimissä verkkokaupoista tai tehdä sopimuksia esimerkiksi puhelinyhtiöön (Tranberg ym. 2013, 95).

8.11. Miten hävität yksityisiä tietojasi sisältävän postin? (esimerkiksi terveystiedot ja muut paperit, joissa henkilötunnus tai muita arkaluontoisia tietojasi näkyy)

Lähes puolet, 46,2 % repii paperit ja laittaa roska-astiaan tai paperinkeräykseen, 26,2 % polttaa, 18,5 % laittaa silppuriin, 3,1 % laittaa roska-astiaan, 1,5 % repii ja laittaa useampaan kuin yhteen roska-astiaan, 1,5 % ei hävitä lainkaan, 1,5 % hävittää työpaikan tietoturva-astian avulla ja 1,5 hävittää muulla tavalla.

Kuten yllä jo mainittiin, henkilötunnuksen avulla voi tehdä useita rikoksia ja täydellisten henkilötietojen avulla rikosten tekomahdollisuus kasvaa.

9 Tutkimus: tositapahtuma fyysisestä identiteettivarkaudesta

Tapaus on osa tutkimusta, jossa tutkimusmenetelmänä on haastattelu. Uhri esiintyy tarinassa ”Uhrina” identiteetin suojaamiseksi. Uhrin tapaus on tapahtunut oikeasti ja kuvataan seuraavassa uhrin omakohtaiseen kokemukseen perustuen. Oikeuden pöytäkirjat ovat salassa pidettäviä, joten niitä ei ole tämän opinnäytetyön liitteenä ja rikoksen tekijästä puhutaan ”Tekijänä”.

Huhtikuussa 2013 Uhrin lompakko varastettiin ruokaravintolasta. Lompakko oli pöydän kulmalla, jossa sitä pidettiin silmällä. Lompakossa oli muun muassa ajo- ja kelakortti ja luottokortti.

Uhri teki asiasta rikosilmoituksen samana päivänä ja kuoletti kaikki kortit. Noin puoli vuotta myöhemmin, syyskuussa 2013 Pasilan poliisiasemalta soitettiin ja Uhrina esiintynyt henkilö oli heillä säilössä. Uhria kuulusteltiin kirjallisesti ja tapahtumat alkoivat selvitä. Tekijä oli ostanut Uhrin ajokortin tuntemattomaksi jääneeltä mieheltä 500 euron kauppahinnalla. Ajokortin avulla Tekijä oli saanut avattua pankkitilin, jonne sai pikavippifirmoilta rahaa Uhrin henkilötunnuksen avulla. Tekijä osti myös puhelimia, iPadeja, kodin tavaroita ja muita tavaroita osamaksulla. Tekijä teki myös Väestörekisterikeskukseen muuttoilmoituksen Uhrin nimissä.

Tekijä jäi kiinni mennessään vuokraamaan yksityishenkilöltä asuntoa. Vuokranantaja alkoi epäillä henkilöllisyyttä, vaikka Tekijä näyttikin Uhrin ajokorttia. Tekijä kirjoitti ensin vuokrasopimukseen oman nimensä, jonka pyyhki yli ja tarkisti sitten ajokortista nimen.

Vuokranantajan epäilykset heräsivät ja Tekijän poistuttua hän soitti poliisille. Tekijälle uskoteltiin, että vuokrasopimuksesta oli jäänyt jokin allekirjoitus uupumaan. Tekijän tullessa allekirjoittamaan sopimusta uudestaan oli poliisi vastassa ja kiinniotto tapahtui.

Vuosi tapahtuneen jälkeen käytiin oikeutta käräjäoikeudessa. Helsingin käräjäoikeus antoi päätöksen 22.10.2014 diaarinumerolla R14/6242. Päätöksenä oli kuusi kuukautta vankeutta ja Tekijä määrättiin maksamaan korvauksina noin 2000 euroa yhteensä kaikille asianosaisille. Tekijää syytettiin 26 eri rikoksesta ja tuomittiin 26 rikoksesta. Kutsu hovioikeuteen tuli 2.4.2015, Tekijä oli valittanut tuomiostaan.
7.4.2015 Uhri sai kirjeen Joensuun poliisilaitoksen löytötavaraosastolta. Kirjeessä kerrottiin poliisin löytäneen Uhrille kuuluvaa omaisuutta. Uhrin kelakortti oli löytynyt maasta Joensuusta. Uhri pyysi poliisia tuhoamaan kortin.

Uhrin nimissä oli asioitu Joensuussa lääkärissä ja saatu lääkemääräys. Tekijä oli antanut tai myynyt kelakortin ystävälleen. Kyseessä olevalla henkilöllä oli useita oikeuskäsittelyitä vireillä ja Uhriin kohdistettu petos jätettiin syyttämättä, koska muita syytteitä oli niin paljon.

Hovioikeudessa Uhrin tapausta käsiteltiin 7.9.2015, kaksi ja puoli vuotta lompakon varastamisen jälkeen. Tekijä ei saapunut paikalle. Hovioikeus kuuli yksityistä vuokranantajaa, jonka ansiosta tekijä oli jäänyt kiinni sekä Uhria. Tuomio pysyi samana. Tapausta käsiteltiin hovioikeuden diaarinumerolla 14/3132.

Rikoksen tekemiseen käytettiin Uhrin identiteettiä ajokortin ja kelakortin avulla. Rikoksen jälkeen Uhri on asettanut osoitetietonsa salaisiksi. Hän harkitsi myös vapaaehtoisen luottokiellon tekemistä ja henkilötunnuksen muuttamista. Henkilötunnuksen muuttaminen oli poliisin mukaan mahdollista, koska henkilötunnuksen väärinkäyttö pystyttiin lukemaan jatkuvaksi ja Uhrille harmia aiheuttavaksi.

Rikoksesta aiheutui Uhrille ansiotulon menetystä 400 euron edestä sekä menetettyä työaikaa. Aluksi Uhri oli shokissa, sitten tunne muuttui peloksi. Pahimmassa tapauksessa rikos olisi vaikuttanut myös Uhrin työuraan, koska hän työskentelee alalla, jolla on myös pankkitoimintaa ja asiakkaat tarkistavat työntekijöiden luottotiedot säännöllisesti. (Uhrin haastattelu.)

9.1. Tutkimustulos

Valitsin Uhrin tapauksen haastattelumenetelmänä, koska tapaus nousi kyselystä esiin. Tapaus oli hyvin mielenkiintoinen, koska se voisi tapahtua kenelle tahansa. Varkaus pääsi tapahtumaan, vaikka normaalia huolellisuutta oli noudatettu. Tapaus noudatti identiteettivarkauksiin liittyvää kaavaa, jossa identiteettiä käytetään vasta jonkin ajan päästä itse rikoksesta. Uhri ei voinut mistään tietää, mitä hänen identiteettinsä avulla oli tehty.

Merkittävää tapauksessa oli Uhrin näkökulmasta pieneksi jäänyt rangaistus. Oikeudessa asianomistajia oli yhteensä 14, eli Tekijä oli kohdistanut rikoksia heitä kaikkia kohtaan. Uhriin liittyviä rikoksia olivat osittain seitsemän petoksen yritystä, joilla Tekijä pyrki hankkimaan oikeudetonta etua tai hyödykkeitä itselleen Uhrina esiintyen. Petossyytteitä oli viisi, yksi kätkemisestä eli Uhrin ajokortin oikeudetta säilyttämisestä, 4 väärennyksestä ja yksi rekisterimerkintärikos osoitteenmuutoksesta. Yhteensä syytekohtia oli 26. Useasta syytteestä huolimatta korvaus Uhrille oli pieni, vain 400 euroa.

Mikäli Tekijä ei olisi syyllistynyt myös muihin rikoksiin, olisi syytekohtana ollut vain kätkemisrikos. Identiteettivarkautta ei oltu vielä kriminalisoitu tapahtumien aikaan, joten emme tiedä, miten tuomio olisi muuttunut, jos myös identiteettivarkaudesta olisi voinut syyttää ja tuomita.

10 Pohdinta

10.1. Tulokset

Tutkimuksessa havaitsin myös turvallisuuden tunteeseen luottamista, joka ilmeni esimerkiksi käyttämällä samaa salasanaa useissa eri palveluissa. Samalla osoittautui, että biometristen tunnisteiden uhat ja haitat eivät ehkä ole kovin hyvin tiedossa tai niihin luotetaan vahvana suojauskeinona välittämättä mahdollisista uhista.

Tutkimus osoitti tutkimukseen osallistuneiden olevan hyvin perillä oman identiteettinsä suojaamisesta ja tietoturvasta. Tutkimukseen osallistuneet edustavat 20-40-vuotiaiden aktiivista sosiaalisen median käyttäjien ryhmää.

Tapaus tosielämän fyysisestä identiteettivarkaudesta oli äärimmäisen mielenkiintoinen ja samalla hyvin ikävä osoitus siitä, miten paljon vahinkoa henkilötunnuksen ja tunnistusasiakirjan joutuminen vääriin käsiin voi aiheuttaa. Tapaus toimii varoittavana esimerkkinä

ja herättää ajattelemaan, mitä itse voisi tehdä oman identiteettinsä suojaamiseksi entistä paremmin.

Opinnäytetyötä tehdessäni tulin itsekin hyvin kriittiseksi omille tavoilleni jakaa tietoa itsestäni sosiaalisessa mediassa sekä tavoistani käyttää eri päätelaitteita. Täysin vainoharhaiseksi tietojensa suojaajaksi ei ehkä tavallisella ihmisellä ole tarvetta, mutta perusasiat kannattaa muistaa ja toimia huolellisesti. Opinnäytetyöni on onnistunut, jos saan sen lukeneet ihmiset muuttamaan yhden omista toimintavoistaan.

Omaa toimintaani muutin aloittamalla eri salasanojen käytön eri palveluissa sekä tekemällä salasanoistani uskoakseni vieläkin turvallisemmat. Lisäksi päätin olla osallistumatta enää kyselyihin. Mietin myös jatkossa tarkemmin, mitä tietoa itsestäni mihinkin annan.

Mielenkiintoinen kysymys nousi mieleeni opinnäytetyötä tehdessäni. Tulevatko identiteettivarkaudet tulevaisuudessa lisääntymään ja miten toimitaan esimerkiksi vakuutusten osalta niiden suhteen? Mikä voidaan osoittaa olevan normaalia huolenpitoa ja mikä on huolimattomuutta?

Oppimisprosessina opinnäytetyön tekeminen mielenkiintoinen ja asetti myös omat ja lähipiirin tavat tarkkailun alle. Aihe osoittautui valtavan laajaksi ja olisi voinut vielä paisua enemmänkin tietoturvan puolelle, jos olisin antanut niin tapahtua. Mielenkiintoista on, miten tulevaisuuden eri älylaitteet, kuten älyvaatteet, -kodinkoneet ja muut vastaavat keräävät ja paljastavat meistä tietoja sekä asettavat meidät aivan uudenlaisen uhan alaiseksi.

Aiheessa oli vaikea pysyä spesifioidusti, koska identiteettivarkaudet ja niiltä suojautuminen koostuvat niin laajasta kokonaisuudesta. Aihetta tutkiessani löysin myös paljon mielenkiintoista tietoa, joka liittyi aiheeseen mutta ei otsikkoon. Mielestäni onnistuin kuitenkin hyvin pysyttelemään asiassa. Sisältö ei ehkä täysin pysyttele otsikon aiheessa, mutta toisaalta identiteetin ympärille muotoutuva verkko on niin laaja, että koin tarpeelliseksi avata työssä laajemmin identiteettivarkauksia.

Tutkimuksessa olisin voinut kysyä vielä joitakin jatkokysymyksiä, kuten onko henkilötunnuksen loppuosan jakamisesta ollut haittaa, uskooko käyttäjä olevansa hyvin suojattu identiteettivarkaudelta ja monia muita. Toisaalta tutkimus ei olisi voinut laajentua kauhean suureksi. Tutkimusta olisi voinut jatkaa vielä mobiilimaksamiseen, eri algoritmien käyttöön, älyvaatteisiin ja -kelloihin, sovellusten synkronointiin, tietosuojaan, liikenteenvalvontaan, sijaintipalveluihin ja moniin muihin tahoihin. Osa näistä vaatisi asiantuntijaosaamista.

10.2. Oppimisprosessi

Pelkäsin ennen kirjoitustyön aloittamista, etten pysty pysyttelemään riittävän laadukkaassa ammattitason tekstin tuotossa. Uskon, että tekstini ei laajentunut liian kerronnalliseksi vaan onnistuin pysymään ammattimaisen tekstin tuotossa. Kirjoitustyötä oli aluksi hieman vaikea aloittaa, koska ei ollut tarkkaa kuvaa siitä, mikä lopputulos tulisi olemaan. Välillä kirjoitustyötä tehdessä tavoite ja lopputulos olivat kirkkaampina mielissä ja välillä himmeämpinä.

Pysyin hyvin aikataulussa, vaikka se oli jo alusta asti melko tiukka. Luulen, että tiukahko aikataulu sopi minulle paremmin ja kannusti tekemään työtä säännöllisesti. Vain yhden kerran työtä tehdessäni tuntui, etten saa mitään aikaan ja lopetin siltä päivältä. Muuten olin aikatauluttanut onnistuneesti arjen lomaan hetket opinnäytetyön tekemiselle ja onnistuin saamaan aikataulussani suunnitellut asiat tehdyksi tuota yhtä kertaa lukuun ottamatta. Uskon, että minulla on kattava näkemys identiteettivarkauksiin ja niiltä suojautumiseen ja tätä olisi mielenkiintoista viedä pidemmälle esimerkiksi hakukoneoptimointiin, data-analysointiin ja eri laitteiden synkronointiin.

Vaikealta tuntui osoittaa uusia näkökulmia tai pyrkiä vastaamaan johonkin tuntemattomaan kysymykseen uudenlaisella tiedolla. Teknologia ja informaatiotiede kehittyvät koko ajan valtavalla nopeudella ja todennäköisesti tämän opinnäytetyön jotkin osiot vanhenevat nopeasti. Ajantasaista tietoa oli vaikea löytää ja muutamassa vuodessa painetut teokset tarjosivat jo vanhentunutta tietoa. Onnistuin kuitenkin mielestäni tuomaan mukaan hyvin ajankohtaisia aiheita ja erityisen tyytyväinen olin oivallukseeni biometrisistä tunnisteista.

Opinnäytetyöni valmistuessa uskon, että identiteettivarkaudelta suojautuminen on sarja toimintatapoja ja osa arkea. Pidä huoli maksuvälineistäsi, identifioivista seikoista kuten henkilöllisyyspapereista ja salasanoista. Älä jaa kaikkea tai jaa kaikki. Tietojen keruuta ei tule pelätä mutta riskit on hyvä tiedostaa. Osa tietojenkeruusta saattaa olla meille jopa eduksi kuten ”Etsi iPhoneni”-toiminto tai sijaintipalvelut esimerkiksi katoamistapauksissa. Molemmat voivat kuitenkin kääntyä myös meitä vastaan. Kuten sananlasku sanoo, tieto on valtaa.

Lähteet

Aktia, Ota verkkopankkitunnukset käyttöön, 2018. Luettavissa: https://www.aktia.fi/fi/verkkopankki/ota-kayttoon Luettu 1.4.2018

Alasuutari P., Laadullinen tutkimus, 1994, s. 23-25.

AVG, Yates, M. 3 Reasons to Never Use Fingerprint Locks on Phones, 12.6.2016. Luettavissa: https://www.avg.com/en/signal/3-reasons-to-never-use-fingerprint-locks Luettu 1.4.2018

BBC, Facebook scandal ”hit 87 million users”, 4.4.2018. Luettavissa: http://www.bbc.com/news/technology-43649018 Luettu 7.4.2018

Det Danske Filminstitut: Horanyi N., En fremmer flytter ind, 2017. Luettavissa: https://www.dfi.dk/en/viden-om-film/filmdatabasen/film/en-fremmed-flytter-ind Luettu 14.4.2018

Ekstra Bladet, Christensen T., Slagelse-bedrager er skingrende gal, 6.2.2009. Luettavissa: https://ekstrabladet.dk/sport/haandbold/article4291153.ece Luettu 14.4.2018

Hallituksen esitys 232/2014, ”Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi” Luettavissa: https://www.finlex.fi/fi/esitykset/he/2014/20140232#idp450086160 Luettu 26.4.2018

Heima T-P., 18.7.2017. Näin voit yrittää välttyä identiteettivarkaudelta – väärillä tiedoilla saa helposti pikavippejä tai lehtitilauksia. Luettavissa: https://yle.fi/uutiset/3-9727894 Luettu 2.3.2018

Horanyi N., Meille muutti vieras mies, 2017. Katsottavissa: https://areena.yle.fi/1-3201606 Katsottu 14.4.2018

Hyytinen T., ”Olet sitä, mistä tykkäät Facebookissa” – Näin poliitikot hyödyntävät luonnettasi mainonnassaan, 29.4.2017 Luettavissa: https://yle.fi/uutiset/3-9584618 Luettu 7.4.2018

Hämäläinen V-P., Tuominen S., 5.11.2017. Joku julkaisi 16 000 suomalaisen henkilötunnukset netissä kuusi vuotta sitten – nyt niillä tehtaillaan tuhansia rikoksia vuodessa. Luettavissa: https://yle.fi/uutiset/3-9914817 Luettu 19.2.2018.

Jyllands-Posten, Manden der fuppede Slagelse, 5.2.2009. Luettavissa: https://jyllands-posten.dk/sport/handbold/ECE4108155/Manden-der-fuppede-Slagelse/ Luettu 14.4.2018

Järvinen P. & Järvinen A., Tutkimustyön metodeista, 2000, 8-9

Järvinen P., Yksityisyys – turvaa digitaalinen kotirauhasi, 2010, s. 25, 35, 164, 172-174, 195, 239, 278

Kangasniemi, Tea 2012. Identiteettivarkaudet – haasteita rikostukinnalle ja -oikeudelle, paljon vaivaa ja harmia uhrille. Luettavissa: https://oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/perus-jaihmisoikeudetrikosprosessissa2012/MIpzV15CB/10_Identiteettivarkaudet_-_haasteita_rikostutkinnalle_ja_-oik..._Tea_Kangasniemi.pdf Luettu 12.3.2018

Karismo A., 15.2.2017. Identiteettivaras vaanii verkossa – Tässä kuusi käytännön ohjetta, joilla vaikeutat huijaajien työtä. Luettavissa: https://yle.fi/uutiset/3-9448910 Luettu 2.3.2018

Keränen T., 19.4.2917. Sormenjäljet ja kasvokuvat yleistyvät tunnistamisessa vaaranmerkeistä huolimatta – "En käytä ennen kuin on pakko". Luettavissa: https://yle.fi/uutiset/3-9561075 Luettu 2.4.2018

Kokkonen Y., 6.4.2018. Facebook: Jopa 2,7 miljoonan eurooppalaisen tiedot annettu Cambridge Analyticalle. Luettavissa: https://yle.fi/uutiset/3-10148233 Luettu 7.4.2018

Kähkönen S., 29.3.2016. Facebook-testeistä voi olla vakava seuraukset – myytkö tietosi ulkopuolisille? Luettavissa: https://yle.fi/uutiset/3-8765560 Luettu 12.2.2018

Leppänen, N. 15.4.2018. Rikoksen uhri. Haastattelu. Hämeenlinna.

Liikenne- ja viestintäministeriön julkaisuja, Ailisto H., Ahonen P., Lindholm M., Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja 15.11.2005 Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78503/80_2005.pdf?sequence=1 Luettu 2.4.2018

mySafety, Research Insight Finland, 31.5.2017. Identiteettivarkaudet ovat Suomessa yleisempiä kuin pyörävarkaudet. Luettavissa: https://www.mysafety.fi/ajankohtaista/identiteettivarkaudet-ovat-suomessa-yleisempia-kuin-pyoravarkaudet Luettu 12.2.2018.

Niiniluoto M., 14/2015. Identiteetin varastaminen on liian helppoa. Luottolista-lehti. Luettavissa: http://www.mynewsdesk.com/fi/asiakastieto/news/luottolista-lehti-identiteetin-varastaminen-on-liian-helppoa-124083 Luettu 12.2.2018.

Pajuriutta Satu, Helsingin Sanomat, 25.2.2017. Muutaman kuukauden seurustelusta seurasi kahdeksan vuoden piina – Poikaystävä vei Minnan, 26, pankkitunnukset ja otti kymmeniä lainoja. Luettavissa: https://www.hs.fi/paivanlehti/25022017/art-2000005102683.html Luettu 1.4.2018

Peltomäki J., Norppa K., Rikos meni verkkoon – näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen, 2015, s. 82, 84, 97, 122

Poliisi, Tietorikoksia, Identiteettirikokset ja kohdistetut hyökkäykset tietorikosten nousevia ilmiöitä. Luettavissa: https://www.poliisi.fi/rikokset/rikosilmioita/tietorikoksia Luettu 1.4.2018

Poliisi, Sähköpostihuijauksia. Luettavissa: https://www.poliisi.fi/rikokset/rikosilmioita/sahkopostihuijauksia Luettu 1.4.2018

Puro, Jessica 2017. Identiteettivarkaus ja sen vaikutukset uhriin. Luettavissa: http://www.theseus.fi/handle/10024/134208 Luettu 12.3.2018

Rikosuhripäivystys 2018. Identiteettivarkaus. Luettavissa: http://www.riku.fi/fi/opaat+ja+ohjeet/identiteettivarkaus/ Luettu: 15.4.2018

Rikosuhripäivystys 2018. Kenelle palvelut on tarkoitettu. Luettavissa: https://www.riku.fi/fi/palvelut/kenelle+palvelut+on+tarkoitettu/ Luettu 15.4.2018

Saastamoinen A., 22.2.2016. Facebook vie yksityisyyden – älä tee sitä liian helpoksi. Luettavissa: https://yle.fi/aihe/artikkeli/2016/02/22/facebook-vie-yksityisyyden-ala-tee-sita-liian-helpoksi Luettu 12.2.2018

Suomen lainsäädäntö 2017. Rikoslaki. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001 Luettu: 12.2.2018.

Suomen Suurlähetystö, Moskova. Sormenjäljet alettiin lisätä uusiin passeihin 29. kesäkuuta lähtien. Luettavissa: http://www.finland.org.ru/Public/default.aspx?contentid=167164&nodeid=36881&culture=fi-FI Luettu 1.4.2018

The Guardian, Davies H. Ted Cruz using firm that harvested data on millions of unwitting Facebook users. 11.12.2015. Luettavissa: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data Luettu 7.4.2018

Tieteen termipankki, Filosofia: identiteetti, 3.4.2018. Luettavissa: http://tieteentermipankki.fi/wiki/Filosofia:identiteetti Luettu 3.4.2018

Tietosuojavaltuutetun toimisto, Biometrinen tunniste, mikä se on? 27.7.2010. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf Luettu 1.4.2018

Tranberg P., Heuer S. Älä kerro kaikkea!, 2013, s. 95, 244-246